A PROPOSED FEDERAL PKI USING X.509 V3 CERTIFICATES

William E. Burr, Noel A. Nazario and W. Timothy Polk
National Institute of Standards and Technology
Gaithersburg MD, 20899

1. Introduction

Public key certificates and digital signatures allow parties who were previously unknown to each other to establish trust relationships and possibly conduct secure, encrypted communications. The Federal Government is a large user community that could greatly benefit from this technology. A public key infrastructure (PKI) is needed to enable broad use of certificates across and among such large user communities.

Early attempts to establish public key infrastructures based on the X.509 public key certificate standard, such as Privacy Enhanced Mail (PEM) [RFC 1422] and the DoD Multi-level Information System Security Initiative (MISSI) [MISSI 95], have defined a hierarchical structure for the infrastructure. Although the hierarchical model is reasonably congruent with the structure of the Government and many other organizations, the primary advantage of the hierarchy was that it provided a convenient way to manage trust and security policies. That is, various branches of the tree have consistent security policies, and the level of trust assigned to a certificate holder can then depend upon the branch of the tree.

As standards for public key certificates evolve, a strict hierarchy is seen as unacceptably inflexible and hierarchical PKIs have not been widely implemented. The "version3" revision to the CCITT X.509 certificate standard [DAM95] extends the certificate with provisions that facilitate explicit management of certificates, certification paths, security policies, and the transfer of trust, so that non-hierarchical infrastructures are now practical and manageable.

This paper describes a proposed structure for a Federal PKI, developed by the Federal PKI Technical Working Group and stated in the Federal PKI Concept of Operations [CONOPS 95], that combines a hierarchy with a more general networked cross-certificate structure. It offers most of the advantages of both systems. A trusted entity that issues public key certificates is called a *certification authority (CA)*. An important attribute of this proposal is that a local CA may issue certificates and broadly cross-certify with whomever it needs, but the certificate holders of other CAs are protected from the possibly unwise cross-certification decisions of that CA.

2. Public Key Certificates

Figure 1 illustrates the X.509 v3 certificate. A certificate includes the issuer name, the subject name and the subject's public key, and is signed with the issuer's private key. If Alice has Bob's certificate, and knows the issuing CA's public key, she can verify Bob's certificate and then use Bob's public key to verify Bob's signature on any document.

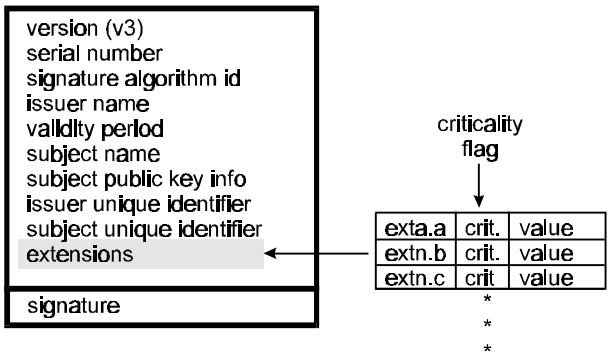

Figure 1 - X.509 Version3 Certificate

Table 1 - Standardized Certificate Extensions

Extension	Used By	Use	Critical (see Note)
Key and Policy Information			
authorityKeyIdentifier	all	identifies the CA key used to sign this certificate	No
keyIdentifier	all	unique with respect to authority.	
authorityCertIssuer	all	identifies issuing authority of CA's certificate; alternative to key identifier	
authorityCertSerialNumber	all	used with authorityCertIssuer	
subjectKeyIdentifier	all	identifies different keys for same subject	No
keyUsage	all	defines allowed purposes for use of key (e.g., digital signature, key agreement...)	Opt.
privateKeyUsagePeriod	all	for digital signature keys only. Signatures on documents that purport to be dated outside the period are invalid.	Opt.
certificatePolicies	all	policy identifiers and qualifiers that identify and qualify the policies that apply to the certificate	Opt.
policyIdentifiers	all	the OID of a policy.	
policyQualifiers	all	more information about the policy	
policyMappings	CA	indicates equivalent policies	No
Certificate Subject and Issuer Attributes			
subjectAltName	all	used to list alternative names (e.g., rfc822 name, X.400 address, IP address...)	Opt.
issuerAltName	all	used to list alternative names	Opt.
subjectDirectoryAttributes	all	lists any desired attributes (e.g, supported algorithms)	Opt.
Certification Path Constraints			
basicConstraints	all	constraints on subject's role & path lengths	Yes*
cA	all	distinguish CA from end-entity cert.	
pathLenConstraint	CA	number of CAs that may follow in cert. path; 0 indicates that CA may only issue end-entity certs.	
nameConstraints	CA	limits subsequent CA cert. Name space.	Opt.
permittedSubtrees		names outside indicated subtrees are disallowed	
excludedSubtrees		indicates disallowed subtrees	
policyConstraints	all	constrains certs. Issued by subsequent CAs	Opt.
policySet	all	those policies to which constraints apply	
requireExplicitPolicy	all	All certs. Following in the cert. Path must contain an acceptable policy identifier	
inhibitPolicyMapping	all	prevent policy mapping in following certs.	
CRL Identification			
crlDistributionPoints	all	mechanism to divide long CRL into shorter lists	Opt.
distributionPoint	all	location from which CRL can be obtained	
reasons	all	reasons for cert. inclusion in CRL	
cRLIssuer	all	name of component that issues CRL.	

NOTE: " "No" means the standard requires the extension be noncritical if used, and "Opt." means that the issuing CA may choose to make that extension either critical or noncritical. "Yes*" means that the standard allows the field to be either critical or noncritical, but the recommendation for the Federal PKI is that it be set to critical. There are no v3 certificate extensions that are required by the standard to be critical.

The optional extensions field is new in the v3 certificate. A certificate can hold any number of extensions. Each extension has a "criticality flag." If a certificate contains a critical extension, a certification path verifier that attempts to verify that certificate must be able to process that extension, or must not verify the certificate. A number of extensions are being standardized [DAM 96]. These standardized extensions are summarized in Table 1. In this paper sans serif type is used to identify the formal names of standardized extensions (e.g., policyConstraints).

3. PKI Organization

Certificates may be chained to form a *certification path*. This is illustrated in Figure 2; Bob has been issued a certificate by CA 3, which has been issued a certificate by CA 2, which in turn has been issued a certificate by CA 1. If Alice trusts CA 1and knows its public key, she can verify each certificate in the certification path until she reaches Bob's certificate and verifies it. At that point, Alice now knows Bob's public key and can verify his signatures.

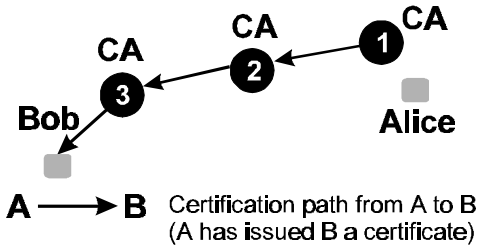

Figure 2 - Certification Path

CAs can certify each other in some systematic manner to form a PKI. A CA may be issued a certificate by another CA. Two CAs may issue each other certificates; this is known as *cross-certification*, and the pair together is a *cross-certificate*. Two alternative PKI topologies, illustrated in Figure 3 below are:

- *Hierarchical*: Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs as illustrated in Figure 3 (a). These CAs may in turn issue certificates to subordinate CAs, or to users. Every user knows the public key of the root CA, and any user's certificate may be verified by verifying the *certification path* that leads back to the root CA. Alice verifies Bob's certificate, issued by CA 4, then CA 4's certificate, issued by CA 2, and then CA 2's certificate issued by CA 1, the root, whose public key she knows;

- *Network*: Independent CA's cross-certify each other, resulting in a general network of trust relationships between CAs. Figure 3 (b) illustrates a network PKI. A user knows the public key of a CA near himself, generally the local CA that issued his certificate, and verifies certificates by verifying a certification path that leads back to that trusted CA. For example, Alice knows the public key of CA 3. There are several certification paths that lead from Bob to Alice, but the shortest requires Alice to verify Bob's certificate, issued by CA 4, then CA 4's certificate issued by CA 5 and finally CA 5's certificate, issued by CA 3. CA 3 is Alice's CA and she trusts CA 3 and knows its public key.

The hierarchical PKI architecture has some advantages. The structure of many organizations such as the government is largely hierarchical and trust relationships are frequently aligned with organizational structure. A hierarchical PKI may be aligned with hierarchical directory names and the certification path search strategy is straightforward. Each user has a certification path back to the root; the user can provide this path to any other user and any user can verify the path, since all users know the root's public key.

It is likely, however, that the strongest reason why early PKIs have been hierarchical is that the hierarchy can be aligned with security policies and this alignment can be used to manage and determine the trust accorded to a particular certification path. While earlier versions of X.509 al-

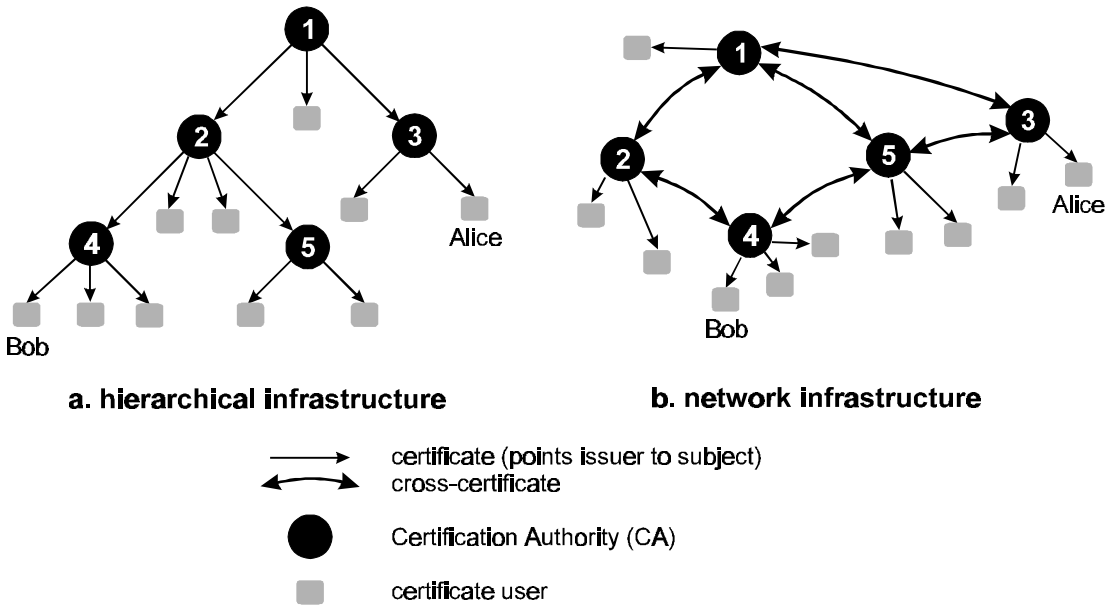

Figure 3 - Alternative PKI Topologies

lowed networks of cross-certified CAs, they provided no mechanism to manage trust in such networks. Version 3 certificates provide alternative means for managing policies and trust.

A strictly hierarchical certification path architecture has some disadvantages. It is improbable that there will be a single root CA for the world, therefore cross-certificates must exist at some level, and certification path verifiers must be able to cope with topologies that are not entirely hierarchical. Commercial and government trust relationships are not necessarily hierarchical, so using the hierarchy itself to manage trust relationships is surely not optimal. Moreover, compromise of the root private key is catastrophic because every certification path is compromised and recovery requires the secure "out-of-band" distribution of the new public key to every user;

The network certification path architecture has the advantage that it is flexible, facilitates ad hoc associations and trust relationships, and readily reflects bilateral trust relationships. It is likely that a national or worldwide PKI will evolve in an ad hoc fashion, from isolated CAs, and this is more easily accommodated in a network than a hierarchy. CAs that are organizationally remote, but whose users work together with a high degree of trust, can be directly cross-certified under a high trust policy that is higher than would be practical through a long, hierarchical chain of certificates. The CAs whose users communicate frequently, can cross-certify directly, reducing certification path processing.

Perhaps the most compelling argument for a network PKI is that it is more convenient and natural for a certificate holder to place his trust in the local CA that issued his certificate, rather than a remote root CA, and make this the foundation of all trust relationships. Moreover, this simplifies the out of band secure distribution of the CA public key and recovery from the compromise of any CA's private key now requires only that the new public key be securely distributed to the holders of certificates from that CA, and new certificates be generated for them.

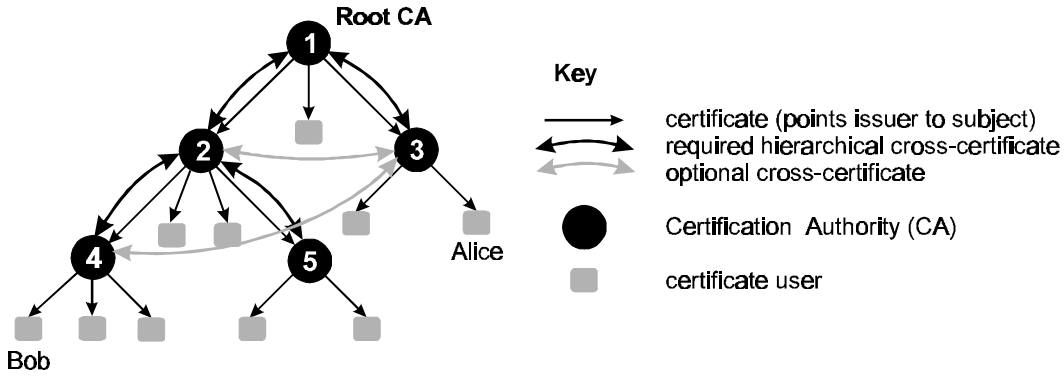

Figure 4 - Proposed Federal PKI Certification Path Architecture

The network PKI has at least two disadvantages: (1) Efficient certification path search strategies are more complex, and (2) a user cannot provide a single certification path that is guaranteed to enable verification of his signatures by all other users of the PKI.

4. Combined Hierarchical-Network Federal PKI

The hierarchical and network PKI architectures are not mutually exclusive. The following hybrid certification path architecture, illustrated in Figure 4, is proposed for the Federal PKI:

- There will be a hierarchical path of certificates leading from the root CA to its subordinate CAs, and from each of these CAs to their subordinates, and so on, until every Federal end user is issued a certificate with a certification path from the root CA;
- Each Federal CA will have a single parent. There will be one or more instance of the directory attribute certificate for certificates issued by the parent. There will be only one hierarchical path to the root CA based on the directory attribute certificate. Other certificates held by a CA, from any other issuer, will be posted in the directory in a crossCertificatePair;
- In parallel to the certificates hierarchically linking CAs to the root will be crossCertificate-Pairs attributes also linking those CAs. These parallel crossCertificatePairs are required and are shown in Figure 4 as black double-headed arrows. This will allow client applications that perform certification path verification from the verifier's parent CA, using the crossCer-tificatePair directory attribute, to operate from any Federal CA;
- Federal CAs may cross-certify each other along paths that do not parallel the hierarchy. Optional crossCertificatePairs are shown in Figure 4 as gray double-headed arrows.

If Alice now wishes to verify Bob's signature, she can find either a certification path that relies on her trust in her parent CA, CA3, or Bob's certification path back to the root. In general, Federal PKI clients and applications may choose to follow either a certification path verification strategy that leads to the root CA, or back to their own CA. Because of the hierarchical cross-certificates, a certification path is guaranteed to exist from her own CA, through the root CA, to every Federal certificate, but there may also be much shorter paths.

5. Federal PKI Management

Some overall management of Federal CAs is needed if trust is to be broadly propagated in an organization as large and diverse as the Federal Government. In this proposal overall management of the Federal PKI is assigned to a Policy Approving Authority (PAA) associated with the root CA. The proposed management principle is to exercise only the central control needed to ensure broad,

consistent transfer of trust throughout the Federal PKI and to limit the damage that holders of certificates from one Federal CA are exposed to as a result of the actions of another CA, while still allowing all Federal CAs broad discretion to serve their users as they see fit.

5.1 Use of V3 Extensions

This proposal uses three extensions to implement government wide management in the Federal PKI:

- certificatePolicies: certification path verifiers compare a list of acceptable policies to the policies listed in the certificate. If there is no match, verification fails. Use of this extension is described in section 5.2 below;
- nameConstraints: this critical extension constrains a CA to issue certificates only for the namespace of specified directory subtrees. Several subtrees can be included. The PAA may use the nameConstraints to restrict namespace for which CAs immediately subordinate to the root may issue certificates, and they may further restrict their subordinates;
- pathLengthConstraint: this component of the critical basicConstraints extension limits the number of certificates that may follow in a certification path. A CA whose certificate pathLengthConstraints value is zero may issue only end entity certificates. The PAA may assign a pathLengthConstraint to certificates issued by the root CA, to limit certification path lengths. Special requirements for cross-certificates are stated in section 5.3, below.

5.2 Policies

We propose that every CA in the Federal will have a PAA approved *operational policy*, governing how the CA is operated (e.g., how the CA private key is protected, how the CA is physically protected, how data is backed up, etc.), and one or more PAA approved *certificate issuance policies*, governing how the CA issues certificates. A principal features of a certificate issuance policy is how the identity of certificate subjects is verified.

V3 certificates allow a policy identifier to be placed in the certificatePolicies extension. If there are many different policies, automatic verification will not be practical. A small set of policy identifiers called *Federal-Assurance-Level-IDs* will be defined (initially, *high*, *medium* and *low*) for Federal use to indicate a relative assurance level, and one of these will be included in the certificatePolicies extension of every FEDERAL PKI certificate. The PAA will evaluate each CA operational policy and certificate issuance policy pair, and determine the highest Federal-Assurance-Level-ID that may be assigned to certificates issued under that policy pair.

5.3 Cross-Certificate Management

Cross-certificates are contained in the directory attribute crossCertificatePair. When CA X cross certifies with CA Y, the directory entry for CA X holds a crossCertificatePair containing two certificates, one called forward, containing the certificate issued by X to Y, and one labeled reverse, containing the certificate issued by Y to X. In Y's directory entry there is a "mirror image" crossCertificatePair.

The essential issue with cross-certificates is how to allow CAs to cross-certify with other CAs to meet the particular needs of their own users, without compromising the security of users of other CAs in the Federal PKI. For example, a particular agency might have a close working relationship with a local government office, a particular contractor, or law firm that has its own CA. That relationship, however, would not necessarily justify extension of trust to other government agencies. To accomplish this three classes of cross-certificates are proposed below for the Federal PKI.

5.3.1 Hierarchical cross-certificates

Hierarchical cross-certificates exactly parallel the hierarchical certification path to the root CA. The forward certificate of each crossCertificatePair for a parent CA is the certificate it issues to the subordinate CA. These hierarchical cross-certificates, shown in Figure 4, are used to ensure that clients that verify certification paths from their own CA, can always find a certification path to any certificate issued in the Federal CA.

5.3.2 General cross-certificates

General cross-certificates supplement the certification hierarchy and allow shorter certification paths. General cross-certificates are governed by rules, described below, so that, when they are used, the propagation of trust is equivalent to the trust that would result from the use of the hierarchical certification paths to the root CA. They are appropriate when cross-certification will shorten the certification paths and improve performance of frequently used paths. In Figure 4, the cross-certificate between CA 2 and CA 3 is a general cross-certificate.

The rule for certificates issued by Federal CAs as part of general cross-certificates is that, before issuing the certificate, the issuer first evaluates the hierarchical certification path from the subject CA to the root CA. It then includes values for certifictePolicies, pathLengthConstraint and subtreesConstraint as follows:

- certificatePolicies: the value of the Federal-Assurance-Level-ID included in a certificate issued as a part of a general cross-certificate is not greater than the lowest Federal assurance level found in the path back to the root.
- pathLengthConstraint: the value contained in a certificate issued as a part of a general cross-certificate is not greater than the path length remaining on the path from the root.
- subtreesConstraint: the values contained in a certificate issued as a part of a general cross-certificate are at least as restrictive as the constraints inherited by the CA along the path from the root. General cross-certification between Federal and non-Federal CAs requires that the certification path to the root CA allow issuance of certificates to non-Federal names.

The effect is that any certification path that includes a general cross-certificate has path length and subtrees constraints at least as restrictive as those imposed through the hierarchical path from the root, and the highest Federal Assurance Level supported by a path using a general cross-certificate is not greater than the highest level supported by the hierarchical path from the root.

5.3.3 Special cross-certificates

Special cross-certificates allow certification paths that do not conform to the restrictions imposed hierarchically along the path from the root CA. Special cross-certificates may only be created between “leaf” CAs, that is CAs with a zero pathLengthConstraint value in all certificates issued to it by other Federal CAs. This blocks further propagation of trust to another CA along the hierarchical certification path. In Figure 4, the cross-certificate between CA 3 and CA 4, both leaf CAs, is a special cross-certificate. A pathLengthConstraint value of zero is included in the two certificates of special cross-certificates to prevent concatenation of special cross-certificates.

Because of the pathLengthConstraint in all the leaf CA’s certificates, only the users of certificates issued by the two CAs participating in the special cross-certificate may use the less restrictive certification path. With special cross-certificates, users of the two CAs may operate under policies allowing a higher trust level or less restrictions than would otherwise be permitted. For example, a CA X, holding a certificate from its parent with a subtreesConstraint that limited its name space

to the Department of Commerce, could cross-certify with a non-government CA. Holders of certificates issued by other government CAs could not use that special cross certificate in Certification paths for two reasons: (1) it violates the subtreesConstraint of CA X's own certificate, and (2) the pathLengthConstraint of CA X's own certificate prevents use of the cross-certificate. Holders of certificates from CA X, who verify certification paths through CA X's public key, would not encounter these constraints.

6. Conclusion

Prior to the advent of v3 certificates, attempts to design large public key infrastructures had featured a hierarchical organization of CAs and certification paths. The main reason for this was to facilitate the management of trust relationships by aligning them with the hierarchy. Certification path verifiers in a hierarchical infrastructure rely on the public key of the root CA. This, however, is an inflexible architecture for large, diverse organizations such as the US Federal Government, and it is difficult imagine how to connect together independent CAs around the world hierarchically. Who would operate the root CA?

The latest revision of the X.509 certificate standard includes several extensions that can be used to manage trust relationships in an architecture of cross-certified CAs, which use client certification path verifiers that rely on the public key of the CA that issued the client his certificate. This is more flexible, and facilitates the growth of an ad-hoc national or international PKI of cross-certified CAs, as needed by individual CAs. It does not, however, automatically provide a framework for coherent overall management of trust relationships in a large organization such as the US Federal Government.

This paper describes a hybrid certification path architecture, developed by the Federal PKI Technical Working Group, that preserves many of the advantages of each architecture, and is proposed for use in a Federal PKI. This architecture uses a hierarchical structure with the new certificate extensions to allow overall management of trust relationships, while giving individual agency CAs the flexibility to cross certify with other Federal and non-Federal CAs as needed to meet the needs of their users. In particular, it prevents unwise cross-certifications of one Federal CA from compromising users of other Federal CAs. It also supports the use of certification path verifiers and trust models that rely on the public key of either the root CA, or the local CA.

7. References

[CONOPS 95] *Public Key Infrastructure (PKI) Version 1 Technical Specifications - Part C: Concept of Operations*, Federal PKI Technical Working Group, Nov. 16, 1995.

[DAM 96] ISO/IEC JTC 1/SC 21 document, *Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, May 20, 1996*.

[MISSI 95] *MISSI Phase 1 Program Overview* , VERSION: 3.3, 17 Oct. 1995.

[POL 95] TWG-95-81, *Technical Security Policy for the Federal PKI*, 25 Aug. 1995.

[RFC 1422] S. Kent, *Privacy Enhancement for Internet Electronic Mail, Part II: Certificate-Based key Management*, IETF RFC 1422, Feb. 1993.

[X.500 93] CCITT Recommendation X.500, *The Directory*, 1993.

[X.509 93] CCITT Recommendation 509, *The Directory: Authentication Framework*, 1993.